(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 041 523 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.10.2000 Bulletin 2000/40

(51) Int. Cl.[7]: **G07F 7/10**, G07C 9/00

(21) Application number: **00302584.8**

(22) Date of filing: **29.03.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **01.04.1999 GB 9907513**

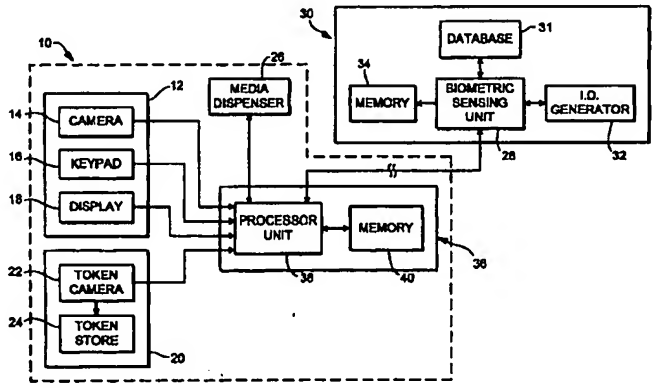
(71) Applicant:
NCR INTERNATIONAL INC.
Dayton, Ohio 45479 (US)

(72) Inventor:
Baird, James Ballantine
Gowrie Park, Dundee DD2 4TW (GB)

(74) Representative:
Williamson, Brian et al
International IP Department,
NCR Limited,
206 Marylebone Road
London NW1 6LY (GB)

(54) Transaction recordal and validation

(57) A method of recording details of a transaction at a terminal comprising the steps: identifying a user at a terminal; the user then instructing a transaction; the terminal retaining an image of a feature of at least one of the user and the transaction; generating a transaction identifier at a remote location; and correlating the transaction identifier with the user identity, the retained image, and at least one feature of the transaction in a respective transaction record. The transaction record may subsequently be reviewed to verify details of the transaction, for example the terminal may retain an image of the user and images of currency deposited in the terminal by the user.



EP 1 041 523 A2

Description

[0001] This invention relates to methods and apparatus for transaction recordal and validation.

[0002] Increasingly, transactions, such as the purchase of goods and the purchase, obtaining or transfer of other valuable media, are carried out via unmanned self-service terminals (SSTs), such as automated teller machines (ATMs). Many SST transactions are "cashless" that is, for example, the user instructs an electronic transfer of funds from a bank account to a vendor. In such transactions the identity of the user may be established and verified by, for example, use of a card bearing a magnetic strip in conjunction with entry of a personal identification number (PIN), or by a biometric identifier such as the iris pattern of the user.

[0003] Difficulties occasionally arise where users claim that transactions have taken place without their knowledge or permission, for example a user may claim that a transaction is erroneous, or was carried out following the theft of a bank or credit card, but before the card issuer was made aware of the theft and the card invalidated. The resulting disputes between customer and financial institution may be acrimonious, and damaging to customer relations.

[0004] In other forms of self-service terminals (SSTs), a user deposits currency or a cheque or voucher in exchange for valuable media, such as a travel ticket. To ensure the deposited currency is genuine, the SST must contain a sophisticated validation system and mechanism. Such systems and mechanisms must be modified from time to time to reflect changes in currency, for example the introduction of new coinage or banknotes, and often encounter difficulties validating older or damaged banknotes. Accordingly, it may prove very expensive to produce and maintain an SST for use in a location, such as an international airport, where it is desired to permit transactions using a range of currencies. Similar problems are encountered with cheque endorsing equipment, where it is desired to allow customers to present cheques in exchange for valuable media.

[0005] It is among the objectives of embodiments of the invention to provide a method and apparatus which obviates or mitigates such difficulties.

[0006] According to the present invention there is provided a method of recording details of a transaction at a terminal, the method comprising the steps:

a user being identified at a terminal;
the user instructing a transaction;
an image of a feature of at least one of the user and the transaction being retained;
a transaction identifier being generated at a remote location; and
the transaction identifier being correlated with the user identity, the retained image, and at least one feature of the transaction in a respective transaction record.

[0007] Subsequently, if a query is raised in relation to the transaction, the transaction record may be retrieved and reviewed.

[0008] The retained image may be of currency, cheques or other tokens deposited by the user, and in this case the transaction record may identify, for example, whether the user deposited valid currency to a value as claimed by the user, as discussed below in greater detail with reference to the second aspect of the invention. Alternatively, or in addition, the retained image may be a feature or image of the user, for example the user's face, and thus by examination of a respective transaction record it may be established whether the user was present when the transaction was executed. Where biometric sensing is utilised in identifying the user, it may be convenient to retain details of the biometric feature or features which serve to identify or verify the identity of the user, for example the user's iris pattern, palmprint, face shape, fingerprint or voice pattern.

[0009] According to a second aspect of the present invention there is provided a method of processing a transaction at a terminal, the method comprising the steps:

a user being identified at a terminal;
the user depositing a token of a claimed value in the terminal and instructing a transaction;
a record of a feature of the token being retained;
a transaction identifier being generated at a remote location; and
the transaction identifier being correlated with the user identity, the recorded token feature and a feature of the transaction in a respective transaction record.

[0010] This aspect of the invention allows an identified user to, for example, purchase valuable media, such as travel tickets, from a terminal which need not include means for immediately verifying the validity of the token, which may be in the form of currency notes, a cheque or voucher. If subsequent validation of the tokens, which may take place at a centralised location, remote from the terminal, identifies that the tokens input into the terminal do not correlate with, for example, the value claimed by the terminal users or the value of the media dispensed by the terminal, the individual transaction records may be analysed to identify that, for example, a user claimed to be depositing 100 currency units and obtained media to that value when in fact only ten units were deposited.

[0011] Such errors or attempted frauds, which are typically relatively infrequent, may thus be detected without the requirement to provide individual terminals with sophisticated and expensive currency validation or cheque endorsing mechanisms or systems.

[0012] Preferably, an image of the token is recorded and retained, it being relatively straightforward to record and store such images digitally or on film. In a preferred embodiment, an image or series of stored images of tokens, for example images of bank notes deposited by a user, may be overlain with the transaction identifier, and possibly other transaction or user identity details, allowing straightforward visual comparison of deposited tokens with recorded transaction details.

[0013] In both aspects of the invention, the user may be identified by first claiming an identity, for example by presenting a magnetic strip card or non-contact card, which claimed identity is then verified by the user by, for example, inputting a personal identification number (PIN) or by the terminal recording a biometric identifier of the user and comparing this with biometric information stored on the card. In such situations the user identity is typically verified by reference to a remote database, or information downloaded to the terminal from a remote database, which identifies whether the claimed identity correlates with the PIN or other information input by or gathered from the user. In other embodiments the terminal may allow a user to be positively identified with reference to a biometric identifier, for example iris pattern, face shape, fingerprint and the like. Again, typically, the user is identified by reference to information stored in or downloaded from a remote database.

[0014] The transaction identifier may be generated at a site operated by a trusted third party where user identification information is stored. The transaction identifier may be stored separately, for example both in a terminal memory or transaction recorder, at or remote from the terminal, and in a user identity record, at or remote from the user identification information storage site, the former typically storing transaction details and the latter user identity details, which information may be subsequently correlated by reference to the common transaction identifier.

[0015] Most preferably, the transaction identifier is relayed to the terminal together with user identity information from a remote user identifying site, and recorded at both locations.

[0016] The transaction identifer may take any appropriate form, and is preferably human readable, such as a sequence of numbers or letters or other symbols. Most preferably, the identifier is a randomly generated code. In other embodiments, the transaction identified may consist of numbers representative of the time and date when the transaction took place, and which number may be combined by user information, for example a user account number. In any event, the time and date of the transaction is preferably stored in at least one record, whether this be the transaction record or a user identity record.

[0017] According to a further aspect of the present invention there is provided apparatus for executing a transaction, the apparatus comprising:

means for identifying a user;

user communication means for accepting user instructions;

processor means for executing a transaction in accordance with user instructions;

means for recording a feature of an image of at least one of the user and the transaction;

means for generating a transaction identifier at a remote location; and

means for correlating the transaction identifier with the user identity, the recorded image and at least one feature of the transaction.

[0018] The user identifying means may take the form of the identifying means found on existing SSTs, for example ATMs, such as a magnetic card reader which allows a user to claim an identity by possession of a particular card, and a keypad which allows input of a PIN by the user to verify the claimed identity. Alternatively, said means may include a biometric sensor for comparing a biometric feature of the user with stored information and thus positively identifying the user. Of course those of skill in the art will identify that there are a wide variety of other systems and methods for identifying or verifying the identity of a user.

[0019] The user communication means may take any appropriate form, including one or a combination of a keypad, screen, touch screen, speech recognition system, natural speech generation system, movement or image sensor, joystick, or mouse.

[0020] The image recording means may take any appropriate form and may comprise one or more of a camera and scanner. The image may be recorded on photographic film or in digital form.

[0021] The transaction identifier generating means may be a random or pseudo-random code or number generator, or may produce sequential codes or numbers, or codes or numbers related to the time or date of the transaction or some other feature of the transaction or user.

[0022] According to a still further aspect of the invention there is provided transaction executing apparatus comprising:

a user identifier;

a user interface;

a processor to implement a transaction in accordance with user instructions input via the interface by an identified user;

an image recorder which records a feature of an image of at least one of the user and the transaction; and

an information store retaining respective transaction records, each record comprising a recorded image, a feature of the transaction and a respective transaction identifier.

[0023] These and other aspects of the present

invention will now be described, by way of example, with reference to the accompanying drawing, which is a box diagram of a self-service terminal (SST) 10 in accordance with a preferred embodiment of the present invention.

[0024] The terminal 10 has a user interface 12, incorporating a number of features and facilities, illustrated as individual modules. In the illustrated embodiment these features include a camera 14, a keypad 16 and a screen 18. The terminal 10 also includes a token receiver module 20 associated with a token input slot (not shown) and comprising a token camera 22 and a secure token store 24.

[0025] The Figure also shows a media dispense module 26 which is associated with a dispenser slot (not shown) in the face of the terminal 10, and a biometrics sensing unit 28 is provided in a remotely located user identifying unit 30 under the control of a trusted third party, also including a biometric information database 31, a transaction identifier generator 32 and memory 34.

[0026] The terminal 10 further comprises a controller unit 36 which communicates with the components of the interface module 12, the media dispense module 26, and components of the user identifying unit 30.

[0027] The controller unit 36 includes a processor 38 and a non-volatile memory 40 implemented by a microcomputer having non-volatile RAM.

[0028] In use, a user approaches the terminal 10 and, following instructions on the terminal face, looks towards the camera 14. An image of the iris pattern of the user is recorded by the camera 14 and a processed iris image is conveyed, via the processor unit 38, to the biometrics sensing unit 28 where the iris pattern data recorded by the camera 14 is compared with the iris pattern data stored in an iris pattern information database 31. Typically, the information stored in the database 31 comprises a collection of individual users's enrolment templates, in the form of iris codes, each representing a processed image of a user's iris. The image received from the camera 14 is processed to create a current iris code, or current template, which is compared with the enrolment templates stored in the database 31 to identify a match and thus identify the user.

[0029] Typically, the enrolment templates, each in the form of a sequence of binary digits, are compared with the current template, also a sequence of binary digits, on a bit-by-bit basis using an exclusive OR function. It is unlikely that a "perfect" match will be achieved, however two templates are considered to match if they differ by less than a predetermined number of bits, the degree of permitted difference being such that the odds of an incorrect match are acceptably low.

[0030] Once the user has been identified by the unit 28, the transaction identifier generator 32 produces a random code, which is stored as an entry in the unit memory 34 together with the user's iris code and note of the date and time. The random code is also relayed to the terminal controller unit 36, together with user data and authorisation for a predetermined range of transactions.

[0031] As noted above, once the user has been identified by the biometrics sensing unit 28, the user is allowed to access certain facilitates provided by the terminal 10 and a menu of the various transactions available to the user may be relayed to the user via the screen 18, user responses being made via the keypad 16.

[0032] By way of example, the user may wish to deposit a cheque in a bank account, and immediately draw cash against the value of the cheque. The user indicates the nature of the transaction by following prompts from the screen 18 and inputting information via the keypad 16, including the value of the cheque. The user then deposits the cheque in the terminal 10, via the token input slot from which the cheque is drawn into the terminal 10 and an image of the cheque is recorded by the camera 22 before the cheque is passed into the token storage 24, which will typically be in the form of a secure cartridge. The requested sum of cash is then retrieved from secure storage by the media dispense module 26 and output from the terminal dispenser slot.

[0033] Details of the transaction are stored as a respective transaction record in the memory 40, together with the images recorded by the camera 22, the record being identifiable by reference to the random code generated in respect of the transaction by the generator 32.

[0034] The terminal 10 will be monitored or visited at frequent intervals to ensure that the terminal contains sufficient media to be dispensed, and also to uplift the token storage cartridge 24. The cartridge 24 is transported to a secure central location where the tokens deposited in the cartridge are be validated; this process will identify any invalid tokens. Further, the total value of the tokens is compared to the value of transactions carried out based on deposited tokens; in the event of a discrepancy between the two totals, the individual transaction records are retrieved from the terminal memory 40 and the recorded images in each record compared to the value of the deposit tokens claimed by the respective users. Once the transaction which is the source of the discrepancy has been identified, the transaction identifier is utilised to locate and retrieve the corresponding record from the user identifying unit as held in the memory 34. This allows the identity of the user responsible for the irregular transaction to be positively identified, the trusted third party responsible for the user identifying unit 30 being able to verify the user identity in the event of any dispute between the user and the terminal operator.

[0035] In other situations, a user may query a transaction which, for example, appears on their bank statement. For example, the statement may show a withdrawal of funds from the user's bank account, of which the user claims to have no knowledge. In this

case the transaction record will contain details of the transaction (but of course no images of deposited tokens), however the transaction identifier code will permit the location and retrieval of the corresponding record from the memory of the user identifying unit, which will positively identify that the user was present and instructed a particular transaction.

[0036] It will be clear to those of skill in the art that the above identified embodiment is clearly merely an example of an application of one aspect of the present invention, and that various modifications and improvements may be made thereto without departing from the scope of the invention.

Claims

1. A method of recording details of a transaction at a terminal, the method comprising the steps:

   identifying a user at a terminal;
   the user instructing a transaction;
   retaining an image of a feature of at least one of the user and the transaction;
   generating a transaction identifier at a remote location; and
   correlating the transaction identifier with the user identity, the retained image, and at least one feature of the transaction in a respective transaction record.

2. The method of claim 1, wherein the retained image includes an image of currency, cheques or other tokens deposited by the user.

3. The method of claim 1 or 2, wherein the retained image includes a feature or image of the user.

4. The method of claim 1, 2 or 3, wherein biometric sensing is utilised in identifying the user.

5. The method of claim 4, wherein the retained image includes a biometric feature used in identifying or verifying the identity of the user.

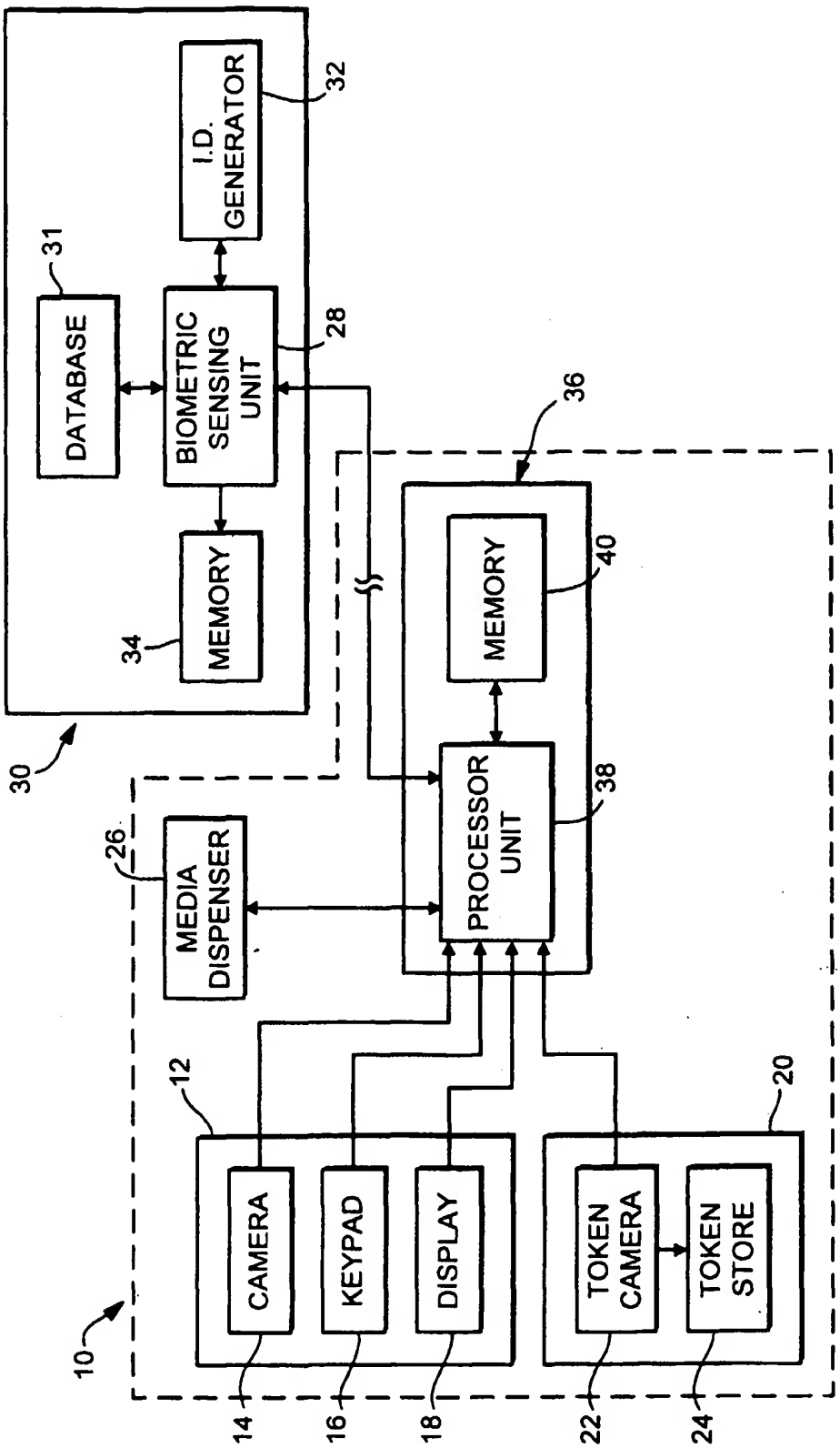
6. The method of any of the preceding claims, wherein the transaction includes the purchase or transfer of valuable media.

7. The method of any of the preceding claims, wherein the retained image is overlain with the transaction identifier.

8. The method of any of the preceding claims, wherein the transaction identifier is stored separately in terminal memory and remote from the terminal in a user identity record.

9. Apparatus for executing a transaction, the apparatus comprising:

   means (14,30) for identifying a user;
   user communication means (16, 18) for accepting user instructions;
   processor means (38) for executing a transaction in accordance with user instructions;
   means (14, 34, 22, 40) for recording a feature of an image of at least one of the user and the transaction;
   means (32) for generating a transaction identifier at a remote location; and
   means (38, 28) for correlating the transaction identifier with the user identity, the recorded image and at least one feature of the transaction.


I.D. GENERATOR
32
31
DATABASE
BIOMETRIC SENSING UNIT
28
36
MEMORY
34
MEMORY
40
30
PROCESSOR UNIT
38
26
MEDIA DISPENSER
12
20
CAMERA
KEYPAD
DISPLAY
TOKEN CAMERA
TOKEN STORE
10
14
16
18
22
24